La población civil en el punto de mira: guerra informativa y manipulación ciudadana. Una aproximación desde el Derecho Internacional[*]

The civilian population in the spotlight: information war and citizen manipulation. An approach from International Law

Chema Suárez Serrano
Doctor en Derecho Internacional Público y Relaciones Internacionales, España
chemasuarez1@gmail.com

Recibido: 05/11/2020 Aprobado: 11/01/2021
DOI: 10.25054/16576799.2784

RESUMEN

Las campañas de desinformación se han convertido en una de las herramientas más utilizadas en los modernos conflictos híbridos, que sustituyen el uso de la fuerza convencional por otros medios tecnológicos, aunque las consecuencias pueden ser similares. Apuntan a los ciudadanos, pero los Estados pagan las consecuencias. Algunas organizaciones internacionales sostienen que vivimos en un estado de guerra informativa, en el que las llamadas noticias falsas (o "fake news") se han convertido en uno de los métodos más recurrentes para estos conflictos no armados. De hecho, a partir del año 2022 los ciudadanos consumiremos más noticias inventadas que reales, pensadas para dirigir la opinión pública contra sus propias instituciones generalmente alterando la voluntad expresada en las elecciones. Es un nuevo método de guerra incruenta, pero con enormes repercusiones para la estabilidad global, representa un desafío que demanda nuevas respuestas. ¿Hasta qué punto las llamadas noticias falsas ponen en peligro la paz y la seguridad mundial? ¿Conviene introducir una nueva categoría de conflictos no armados? Y la más elemental de todas, ¿estamos en situación de guerra o paz?

PALABRAS CLAVE

Conflictos Armados; Conflictos Híbridos; Desinformación; Noticias Falsas; Libertad de Expresión.

ABSTRACT

Disinformation campaigns are one of the most widely used tools in modern hybrid conflicts, which replace the conventional force to other technological means, although the consequences can be similar. They target citizens but states pay the consequences.

[*] Artículo de investigación.

Some international organizations maintain that we live in a state of information war, in which the so-called fake news have become one of the most recurrent methods for these non-armed conflicts. In 2022 at the latest, citizens will consume more invented than real news, designed to direct public opinion against their own institutions, by altering the will expressed in the elections. We are facing a new bloodless warfare with enormous repercussions for global stability, a challenge that demands new responses. To what extent does the so-called fake news endanger world peace and security? Should a new category of non-armed conflict be introduced? And the most elementary of all, are we in a situation of war or peace?

KEYWORDS

Armed Conflicts; Hybrid Conflicts; Disinformation; Fake News; Freedom of Expression.

INTRODUCCIÓN

Debemos, para empezar, matizar a qué nos estamos refiriendo cuando hablamos de "noticias falsas" ya que resulta una expresión contradictoria. Noticia, por definición, es un acontecimiento nuevo y verdadero, mientras que *noticia falsa* resulta ser un oxímoron acuñado precipitadamente para designar el problema del que nos vamos a ocupar. Instituciones nacionales e internacionales, así como la amplia mayoría de los investigadores que abordan este fenómeno desde distintas perspectivas lo hacen con el nombre genérico de desinformación *(disinformation)*, a pesar de que entre los ciudadanos e incluso en el argot de los medios de comunicación se ha popularizado el sintagma *noticias falsas* y más aún su versión en inglés *fake news* (Fundéu RAE, 2017). Obviamente, el objetivo de este trabajo no es la aclaración nominal de un concepto sino el concepto en sí: las operaciones maliciosas de manipulación para influir en los ciudadanos mediante la difusión de mensajes falsos con la intención de obtener beneficio particular. Pero necesitamos un nombre por el rigor que requiere el lenguaje científico, así que lo llamaremos *desinformación* ya que como se ha dicho, es la expresión preferida por la academia, si bien con algunos matices.

Una referencia ampliamente utilizada por su claridad (Consejo de Europa, 2017) distingue entre la información falsa voluntariamente difundida para causar daño *(Dis-information)*, información falsa que por su escasa relevancia apenas afecta a sus protagonistas (*Mis-information*), y la información verdadera que se difunde con la intención de dañar (*Mal-information*). Tampoco podemos defender la originalidad de esta investigación en sentido literal, porque la desinformación como práctica para lograr objetivos políticos o militares no es nueva. Enseguida veremos que existe desde tiempo inmemorial y al igual que la doctrina militar, ha ido perfeccionado sus métodos particularmente desde la Segunda Guerra Mundial (Levin, 2016).

Su funcionamiento básico es invariable y muy simple: son operaciones (abiertas o secretas) diseñadas para favorecer a alguna de las partes en litigio mediante la manipulación informativa que termina modificando la posición de los ciudadanos sin que lo perciban así. Al contrario, creen que actúan siguiendo su

libre voluntad y en el ejercicio de unos derechos que protegen las democracias contra las que se rebelan sin darse cuenta (este es el objetivo del ataque). Lo verdaderamente original ahora es el uso de la desinformación a gran escala con un elevado alcance imposible antes. La desinformación y el engaño siempre han formado parte de los conflictos convencionales pero su influencia se ha acrecentado exponencialmente como parte esencial de las modernas guerras híbridas.

Otro aspecto novedoso es la consideración formal de este problema como amenaza para la seguridad de los Estados. Los gobiernos contemporáneos ya sitúan la desinformación y las interferencias en los procesos de participación política de los ciudadanos entre los principales desafíos para su propia seguridad (D. 14/2019.). ¿Y cómo hacen frente? Por el momento las reacciones se están produciendo todavía de manera desordenada y poco efectiva, tanto individual (cada Estado por su cuenta) como conjuntamente dentro de las Organizaciones Internacionales, y generalmente en una doble dirección. Primero, con la implementación de normas que tratan de obstaculizar la difusión de la desinformación que según la Asamblea General de las Naciones Unidas (ONU) tensan peligrosamente los límites que protegen la libertad de expresión de los ciudadanos (ONU 2020b), y segundo sencillamente avisándonos para que estemos atentos, reconociendo públicamente que estamos sumidos en lo que la Unión Europea llama un estado de *guerra informativa* (Parlamento Europeo, 2016).

Aquí hemos llegado por un uso malévolo de la confianza de los ciudadanos y de las modernas herramientas digitales, utilizadas para legitimar acciones que amenazan la soberanía, la independencia política y la integridad territorial de los Estados, peligros de gravedad suficiente que justifican el estudio concienzudo de este problema. Dicho de otro modo, la desinformación vulnera uno de los principios elementales del Derecho Internacional, como es la abstención de interferir en los asuntos de otro Estado, íntimamente ligado al que defiende la igualdad soberana de todos ellos.

Hace medio siglo que la Asamblea General de la ONU declaró cualquier actuación sobre la independencia política de alguno de sus miembros contraria a los principios y propósitos de la Organización, que como se sabe, se centran en el mantenimiento de la paz global (ONU, 1970). La desinformación aparece como una forma de injerencia en la soberanía, atenta contra la convivencia pacífica, contra el derecho de los ciudadanos a la libertad de expresión, a recibir información veraz y útil, y paralelamente levanta dudas sobre la validez de las herramientas empleadas para combatirla. En muchas ocasiones la reacción de los Estados para protegerse erosiona más los derechos de sus nacionales que la agresión recibida

El efecto de la desinformación y sus consecuencias para la paz y seguridad internacionales también figura en la agenda de la ONU, que pide a los Estados responsabilidad en el uso de estas operaciones y la observación de las normas de Derecho Internacional Humanitario cuando se emplean en el transcurso de un conflicto armado. La magnitud que está tomando el problema abre otras interrogantes: ¿La difusión de desinformación a gran escala supone

realmente una amenaza para la paz y seguridad? ¿Una campaña de desinformación contra un Estado puede considerarse un ataque? ¿Daría lugar a la aplicación del Derecho Internacional Humanitario? ¿Los mensajes falsos son armas? ¿Pueden ser señalados como objetivo militar? La velocidad del mundo digital ha venido a complicar las cosas.

La era de internet representa un avance a escala global para el ejercicio de las libertades públicas, sin embargo, cada vez con mayor frecuencia aparece la duda sobre si también supone una amenaza para la democracia. Numerosas iniciativas jurídicas, políticas y ciudadanas lo debaten con inquietud y promueven el pensamiento crítico ante la avalancha de mensajes que recibimos cada día. A todo esto, los gobiernos juegan a dos barajas porque mientras elaboran planes para defendernos de la desinformación, invocan las fake news (o las utilizan sin escrúpulos) para deslegitimar los mensajes contrarios a sus intereses o a los periodistas críticos con su gestión. El temor crece en la cercanía de un proceso electoral, cuando se producen las más severas acometidas aprovechando la especial sensibilidad del electorado como demuestra la reciente Resolución del Parlamento de la Unión Europea que alerta sobre la avalancha de ataques a través de mensajes malintencionados para influir en las elecciones de los Estados miembros (European Parliament, 2019).

¿Votamos libremente o manipulados? ¿Hasta qué punto nuestras opiniones realmente son propias y no adquiridas? Un número creciente de personas en todo el mundo muestra su preocupación por la autenticidad de la información que consumen principalmente en tiempo de elecciones (World Forum for Democracy, 2019) y ya se anticipa que en 2022 los ciudadanos consumiremos más noticias falsas que verdaderas (Panetta, 2017). La necesidad de mantener informada a la población aparece en la Agenda 2030 impulsada por las Naciones Unidas para cumplir con los 17 objetivos de desarrollo sostenible, pero en el mundo actual se tambalea el equilibrio entre información y democracia, se ataca la conciencia de los civiles en tiempo de paz, pero sin armamento convencional. Los ciudadanos se convierten en enemigos de sus propios Estados y simultáneamente en víctimas de la manipulación informativa difundida principalmente por internet, ese espacio global que nos hace más libres, ese lugar difuso donde la mentira se propaga más rápidamente que la verdad. Más adelante veremos por qué.

1. EVOLUCIÓN HISTÓRICA DE LA DESINFORMACIÓN

1.1. Una herramienta útil para la guerra.

La mentira es un arma legal para la guerra, aceptada y utilizada por los contendientes desde tiempo muy lejano. Ya la edad media Sun Tzu ya advertía a los estrategas militares sobre la importancia del engaño como valiosa estrategia para conseguir la victoria militar: “Una operación militar implica engaño. Aunque seas competente, aparenta ser incompetente. Aunque seas efectivo, muéstrate ineficaz...” (Cleary, 2008, p. 25). Y así se ha seguido haciendo hasta nuestros días, con la evolución marcada por los tiempos y las posibilidades técnicas. Karl Von

Clausewitz ya sabía a principios del siglo 19 que en las campañas militares es más importante cuidar las formas que el fondo, el *cómo* se hace es más relevante que el *qué* se hace.

Durante la guerra de Secesión de los Estados Unidos de América (1861-1865) los ejércitos observaban las normas sobre conducción de hostilidades elaboradas por el jurista Francis Lieber que contemplaban el engaño como método de guerra (Lieber, 1863). El llamado *Código Lieber* recogía la práctica general de los ejércitos e influyó en la posterior positivación del Derecho Internacional Humanitario. Se habla de estratagemas en la Declaración de Bruselas[1] de 1874, o en las primeras Convenciones de La Haya de 1899 y 1907, que declaran como lícitos los ardides de guerra y el empleo de los medios necesarios para despistar al enemigo. Similar provisión figura en las normas sobre derecho consuetudinario (ICRC, 2005), que autorizan el engaño y las estratagemas porque no infringen ninguna regla del Derecho Internacional Humanitario.

Igualmente, el Protocolo Adicional 1 a los Convenios de Ginebra (1977) recoge de manera explícita la validez de las informaciones falsas[2], convirtiendo la mentira en una recurrente herramienta legal. Engañar, simular, despistar, manipular información... Son prácticas que no vulneran ninguna norma de derecho internacional, ni son pérfidas ya que no apelan a la buena fe del adversario. Hasta principios del siglo 20 el engaño formaba parte de campañas muy localizadas dirigidas a confundir al enemigo en el campo de batalla y en momentos puntuales, pero a partir de entonces también se orientan hacia los ciudadanos, precisamente cuando los estrategas apreciaron la importancia del apoyo público para el éxito militar.

La Primera Guerra Mundial supuso una importante inflexión como el primer gran acontecimiento informativo de relevancia mundial que suscitó enorme interés entre la población y espoleó el ejercicio del periodismo. Hasta ese momento las Relaciones Internacionales eran parcela reservada sólo para los gobiernos ya que el tiempo necesario para la difusión de las crónicas o la dificultad técnica para difundirlas, junto con la escasa alfabetización de los ciudadanos obstaculizaban la emisión de información (Pizarroso, 2007); pero el primer enfrentamiento bélico mundial convirtió a los medios de comunicación y a la opinión pública en actores internacionales –y más aún a partir de la Segunda Guerra Mundial- capaces de influir e incluso alterar el desenlace de los conflictos armados.

Desde entonces el desarrollo de las operaciones bélicas ha dependido progresivamente del manejo de la opinión pública más que de la acción de los ejércitos en campaña (Payne, 2005) La Unión Europea llama a este proceso *guerra informativa* y apunta que es un fenómeno histórico tan antiguo como la propia guerra convencional (Parlamento Europeo, 2016) aunque no se generalizó hasta el siglo 20 durante la Guerra Fría para en adelante convertirse en parte intrínseca de las llamadas *guerras híbridas* modernas.

Si la mentira ha servido al esfuerzo bélico desde tiempo inmemorial utilizando principalmente prensa radio y televisión, es fácil imaginar su impacto

[1] Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874: Art. 14. “Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country (excepting the provisions of Article 36) are considered permissible.”

[2] Artículo 37. 2. Protocolo 1 a los Convenios de Ginebra (1977).

con las posibilidades que traía internet. El mundo digital amplifica el efecto del engaño y lo difunde hasta niveles jamás imaginados involucrando a los ciudadanos sin su consentimiento, pero con su necesaria colaboración. El objetivo de semejantes ataques es desestabilizar la situación política, económica y social del Estado atacado sin que parezca una guerra y desde luego sin declaración formal. Todos los gobiernos negarán hacer uso de estas maniobras de ataque, pero todos incluyen ya las operaciones de engaño y desinformación en sus instrucciones militares mientras que el llamado *Manual de Tallin* (Schmitt, 2017) sobre la aplicación del Derecho Internacional en el ciberespacio, elaborado a instancias de la OTAN, defiende su legalidad en la esfera virtual.

La guerra se desborda, adopta nuevas formas y nos abraza a todos sin importar que seamos civiles, o que estemos en tiempo de paz. La Unión Europea Comisión Europea en una de sus aproximaciones más recientes sobre la desinformación contemporánea nos ayuda a comprender su alcance:

> Información verificablemente falsa o engañosa que, de forma acumulativa, (a) se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población y (b) puede causar un perjuicio público, entendido como amenazas contra los procesos democráticos políticos y de elaboración de políticas, así como contra los bienes públicos, como la protección de la salud, el medio ambiente o la seguridad de los ciudadanos de la UE. (European Commission, 2019a, p.1).

La legalización secular de la mentira como arma de guerra nos ha traído hasta aquí. La civilización avanza, pero el siglo 21 no ha eliminado la barbarie, sólo la ha perfeccionado, que diría *Voltaire*.

1.2. Desinformación y fake news, un asunto de dominio público

Aunque los Estados llevan décadas perfeccionando sus estrategias *desinformativas* de ataque y defensa, la incorporación del término "noticias falsas" en el debate público ha sido muy reciente y ocurre como consecuencia de su aparición en el discurso político, primero en Estados Unidos e inmediatamente después en Europa y particularmente tras su influencia en el referéndum que determinó en 2016 la salida del Reino Unido de la Unión Europea o en las posteriores campañas electorales que se van sucediendo actualmente en los países europeos. El referéndum constitucional en Italia (2016), las presidenciales en Francia (2017) o las elecciones al Parlamento Europeo (2019) (Barrancos, 2019) son otros ejemplos en nuestro entorno cercano.

Piense en la cantidad de veces que lo hace, seguro que también usted ha incorporado la expresión "noticias falsas" a su jerga cotidiana. No en vano fue candidata a palabra del año 2017 (Fundéu RAE, 2017), posición que sí obtuvo su versión inglesa "fake news" en el Reino Unido según el diccionario *Collins*, y un año antes, 2016, la palabra "post-truth" (posverdad) en los diccionarios *Oxford*, término adoptado

por la Real Academia Española en 2017. En todos los casos, estas prestigiosas publicaciones habían observado un notable incremento del uso de estas palabras entre la población y los medios de comunicación, contagiados por el debate político y el impulso de las llamadas redes sociales, que actúan como primeros facilitadores de la desinformación (Althius & Strand, 2018).

Paralelamente, los principales sitios web de intercambio de mensajes comenzaban a tomar conciencia sobre la necesidad de limitar la actividad a grupos que difunden información falsa. En los días previos a las elecciones al Parlamento Europeo de 2019 *Facebook* llegó a identificar y eliminar más de 500 páginas o grupos que empleaban tácticas de desinformación. En total, su contenido habría superado los 500 millones de visualizaciones en toda Europa, con más de 6 millones de seguidores, e igualmente repitieron la operación durante la campaña electoral en Estados Unidos 2020. *Facebook, Google y Twitter* han suscrito un código de conducta para evitar la difusión de este tipo de mensajes en internet, recogido por la Comisión Europea (2019) en su alerta sobre el riesgo que acecha a la libertad de expresión:

> As the Commission repeatedly acknowledges in the Communication, the Signatories are mindful of the fundamental right to freedom of expression and to an open Internet, and the delicate balance which any efforts to limit the spread and impact of otherwise lawful content must strike (European Commission, 2019b, p.1).

A continuación, aparece el *Plan de Acción contra la Desinformación* (Comisión Europea, 2018) que reconoce la existencia de la guerra informativa y el riesgo que supone para los valores que defiende la democracia. Había un sonoro antecedente en las elecciones presidenciales en Estados Unidos que ganó el candidato republicano Donald Trump en 2016 (situación repetida en las recientes elecciones de 2020) precisamente el año en que comienza la era de la posverdad (Haiden, 2018) en la que estamos sumidos.

2. LA DESINFORMACIÓN COMO AMENAZA PARA LA PAZ Y SEGURIDAD

2.1 ¿Una amenaza real?

La mentira se propaga más rápidamente que la verdad en internet. Según un estudio que toma como base los mensajes difundidos por Twitter entre 2006 y 2017 (Soroush, Deb & Sinan 2018) las informaciones falsas se difunden hasta cien veces más que las verdaderas y de forma más rápida. Las historias falsas inspiran miedo, disgusto o sorpresa en las respuestas de los usuarios, al tiempo que las verdaderas provocan tristeza, alegría y confianza. Sin embargo, contrariamente a lo que se pensaba, los robots aceleran la difusión de ambas en igual medida que las personas, lo que quiere decir que somos nosotros quienes difundimos desinformación con más celeridad y empeño. Piense otra vez: ¿Cuántas veces habrá difundido sin saberlo contenido malicioso preparado para debilitarnos? El mismo estudio dice que los ciudadanos somos colaboradores necesarios para la extraordinaria repercusión de los mensajes falsos, que gracias a nosotros tienen un 70% más

posibilidades de propagación que uno verdadero.

Ocho de cada diez ciudadanos europeos opinan que las llamadas noticias falsas suponen una amenaza para la democracia, mientras que siete de cada diez usuarios de internet desconfían de la veracidad de la información que publican los medios de comunicación en tiempo de elecciones (European Commission, 2018b) Estos datos revelan que el debate sobre las "fake news" ha alcanzado de lleno a la población, y sobre todo que estamos tomando conciencia del peligro que suponen. ¿Pero realmente son una amenaza para la paz o seguridad en el sentido jurídico? Resolver esta cuestión es una de las claves para su abordaje porque la catalogación oficial de una situación como *amenaza* determinará la solución.

Como se sabe, el Derecho Internacional otorga al Consejo de Seguridad de la ONU la facultad para señalar la existencia de *toda* amenaza a la paz, quebrantamiento de la paz o acto de agresión, según consta en el artículo 39 de la Carta de San Francisco. La paz del mundo depende de la eficaz localización y neutralización de las amenazas que la ponen en peligro, siendo el máximo órgano ejecutivo de la ONU el encargado de tan ardua tarea que representa la piedra angular del sistema de las Naciones Unidas, cuya importancia y singularidad aparecen también recogidas en el primer artículo de la Carta:

> Artículo 1: "Los propósitos de las Naciones Unidas son: Mantener la paz y la seguridad internacionales, y con tal fin: tomar medidas colectivas eficaces para prevenir y eliminar amenazas a la paz…" (ONU, 1945a).

Sin embargo, partimos de una base difusa porque no existe en el Derecho Internacional una definición más precisa sobre este concepto, de manera que *amenaza* será lo que así interprete el Consejo de Seguridad cuya posición depende de factores muy diversos según el momento o los actores implicados. De hecho, las situaciones que han merecido la etiqueta formal de amenaza a lo largo de los años han sido muy diversas y casi inabarcables (Gutiérrez y Cervell, 2012). Desde la persistencia de un conflicto armado interno, como ocurrió durante la guerra de los Balcanes (1991), Angola o Ruanda, la represión de la propia población provocando riesgo de éxodo masivo (Iraq 1991), la implicación en actos de terrorismo internacional (1992), las violaciones masivas del Derecho Internacional Humanitario y los Derechos Humanos durante un conflicto armado (1993), un gobierno golpista (Haití 1994) o el despliegue militar en las fronteras de un Estado vecino (Iraq 1994).

Ya en el siglo 21 el Consejo ha visto amenazas para la paz en la dejación de un Estado de su responsabilidad de proteger a su población (Libia 2011), el tráfico ilegal de pequeñas armas (2015), el cultivo, la producción, el tráfico y el consumo ilícitos de estupefacientes (2019), o las actividades terroristas del llamado Estado Islámico (2919). Todas estas situaciones son oficialmente amenazas en su plenitud jurídica y pueden desencadenar las respuestas que contemplan los tratados. Pero su peso específico no se queda aquí, y el concepto de amenaza como riesgo para la paz también es el primero de los

Principios de Derecho Internacional declarados por la Asamblea de la ONU en su célebre Resolución 2625, hace ya medio siglo (la cursiva es añadida):

> Todo Estado tiene el deber de abstenerse en sus relaciones internacionales de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o *en cualquier otra forma* incompatible con los propósitos de las naciones Unidas. (Asamblea General de la ONU, 1970).

2.2. Hacia la declaración de la amenaza

Visto el impacto de la desinformación sobre la independencia política de los Estados, ¿podríamos interpretar que las informaciones falsas son esa *cualquier otra forma* de amenaza incompatible con la Carta que recoge este principio? La Asamblea General de la ONU ya lo ha considerado así en su novedosa alerta sobre la creciente utilización de las nuevas tecnologías de la información y las comunicaciones como *instrumentos de guerra* por parte de los Estados, para recordarles:

> El deber que tienen de combatir la difusión de noticias falsas o distorsionadas que puedan interpretarse como una injerencia en los asuntos internos de otros Estados o como perjudiciales para la promoción de la paz, la cooperación y las relaciones amistosas entre Estados y naciones, reconociendo el deber de un Estado de abstenerse de toda campaña de difamación, vilipendio o propaganda hostil que tenga por fin intervenir o injerirse en los asuntos internos de otros Estados (Asamblea General de la ONU, 2018).

Los bloques políticos del mundo se posicionan sobre este fenómeno con claridad meridiana. Por su lado, la Unión Europea alerta sobre el peligro que encierran las campañas de desinformación en línea e igualmente Estados Unidos, China o Rusia la consideran desde tiempo reciente como uno de los principales riesgos externos que amenazan su seguridad. También la OTAN ha incluido las informaciones falsas dentro de las amenazas híbridas cuya desactivación sitúa entre sus prioridades por su potencial desestabilizador, y del mismo modo la Comisión Europea se ha pronunciado ya sobre la amenaza en evolución que representa la desinformación debido a su influencia negativa en los procesos democráticos y el debate ciudadano. Tampoco en los conflictos híbridos es fácil marcar el concepto de amenaza con precisión, si bien puede haber situaciones que pongan en peligro la paz y la estabilidad mundial y en esos casos claramente lo son (Schmitt, 2017).

Parece claro que la consideración de la desinformación como amenaza con todas sus implicaciones jurídicas ya está en la agenda de las Organizaciones Internacionales, en las doctrinas militares, en las estrategias de seguridad de los Estados, entre las preocupaciones de la población, y ahora también en la práctica de las grandes empresas de seguridad digital. Estas compañías ya han situado las interferencias en las

elecciones entre las principales amenazas para la seguridad global y consideran la desinformación vertida en las redes sociales como el principal foco de riesgo (Symantec, 2019).

Pero lo cierto es que ninguna de las operaciones de desinformación conocidas hasta ahora ha sido catalogada como amenaza en el sentido jurídico, algo que considerando la discrecionalidad del Consejo de Seguridad de la ONU no sería descabellado pensarlo a medio plazo. Podría ser cuestión de tiempo, y si esa posición no ha llegado aún quizá sea porque las campañas de desinformación planteadas hasta ahora no han alcanzado la magnitud suficiente, o quizá porque actualmente la planificación de los ataques más agresivos con mensajes manipulados sólo está al alcance de los Estados más poderosos y desarrollados tecnológicamente, muchos de los cuales tienen asiento permanente en el Consejo de Seguridad o lo que es lo mismo, la posibilidad de vetar una Resolución semejante.

3. LA DESINFORMACIÓN COMO ATAQUE O ACTO DE AGRESIÓN

De acuerdo con el artículo 49 del Protocolo Adicional 1 a los Convenios de Ginebra, un ataque es un *acto de violencia* contra el adversario, sea ofensivo o defensivo. El uso de la violencia está implícito en el concepto mismo de ataque, de lo que se deduce que las acciones que no la ejerzan, como un ciberataque, no serán considerados como tal (a pesar de su nombre) a menos que se encuadren dentro de una operación que suponga el uso de la fuerza, y sólo en esos casos estarán sujetas a las reglas del Derecho Internacional Humanitario, según la posición defendida por el Comité Internacional de la Cruz Roja (ICRC, 2015).

Pero igual que ocurre con la designación oficial de la amenaza, también es el Consejo de Seguridad de la ONU el órgano competente para determinar qué es un acto de agresión (según dispone el artículo 39 de la Carta que hemos nombrado ya) y decidirá qué acciones tomar para contrarrestarlo cuando se produzca.

Contrariamente al concepto de amenaza, del que no tenemos una definición precisa, el acto de agresión sí está parcelado de manera clarificadora reduciendo el margen de interpretación del Consejo. Aparece en la Resolución 334 (XXIX) de la Asamblea General (1974), donde leemos que se entiende por agresión el uso de la *fuerza armada* por parte de un Estado en contravención de la Carta de la ONU. Luego enumera algunos ejemplos como la ocupación militar, el bombardeo o el bloqueo de puertos, pero avisa que el listado no es exhaustivo y deriva al Consejo la facultad para determinar qué otras situaciones pueden merecer la misma consideración en el futuro. Hoy día, medio siglo después, resulta difícil definir un acto de agresión en las guerras del siglo 21, dominadas por el componente híbrido multidisciplinar en las que el uso de la fuerza generalmente no existe, lo cual ha abierto una laguna conceptual que no ayuda a parcelar el problema.

En el ámbito penal, los signatarios del estatuto de la Corte Penal Internacional necesitaron más de 10 años para llegar a un acuerdo sobre la definición jurídica

del acto de agresión, que no aparece entre sus competencias una enmienda introducida en 2010 para copiar la posición que tres décadas antes había fijado la Asamblea General de la ONU: "Agresión es el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas" (ONU 1945b).

¿La injerencia en los asuntos internos de un Estado mediante la manipulación informativa podría considerarse como *cualquier otra forma* incompatible con la Carta? El uso de la fuerza y la violencia física siguen siendo premisa general para la identificación del acto de agresión y esto reduce significativamente las posibilidades de colgar esta etiqueta a la desinformación. Las reduce, sí, pero no las elimina por completo porque hoy está comúnmente aceptado que la violencia de un ataque no depende tanto de los medios como de sus consecuencias.

Pensemos por ejemplo en el empleo de agentes biológicos, químicos o radiológicos. Está por encima de toda duda que estos métodos suponen un ataque violento, aunque no vengan acompañados de la fuerza convencional (Droege, 2012). El umbral lo marca el grado de sufrimiento de la población, de manera que si los efectos sólo son incomodidades pasajeras o una leve disminución de la calidad de vida no puede hablarse de un ataque con propiedad, pero si se producen otras situaciones de mayor envergadura aún sin fuerza armada, como un colapso de la economía, del sistema democrático, aumento del desempleo, ansiedad generalizada entre la población, miedo, pánico u otras situaciones de similar gravedad, sí podría ser tomado por ataque en toda regla (Schmitt, 2002).

3.1. Un problema presente con efectos a largo plazo

A la hora de designar la gravedad de una acción no sólo cuentan sus efectos presentes, también los futuros porque si encierra un peligro latente que previsiblemente provocará a medio plazo daños graves a personas o lugares protegidos también estaremos ante un ataque, aunque no se apoye en la violencia convencional. Algunos episodios recientes muestran la posibilidad de que la desinformación configure un escenario de esta naturaleza, como las pérdidas millonarias que ocasionó la difusión de mensajes falsos sobre la muerte en accidente de tráfico en 2017 del fundador de *Ethereum* una de las más valoradas criptomonedas, e igualmente ocurrió con la difusión del mensaje falso sobre la muerte por Covid-19 del primer ministro británico Boris Johnson en 2020, que diferentes medios de comunicación en todo el mundo dieron por verdadero.

¿Podría ocurrir con la información maliciosa, diseñada intencionalmente para dañar la credibilidad del Estado, la calidad de la democracia, o para minar la moral de la población y su confianza en las instituciones? La difusión de propaganda o la guerra sicológica e incluso económica siempre han estado excluidas de la definición de ataque (Bothe, 1982) y verdaderamente parece difícil rebatir con los argumentos jurídicos que hoy disponemos. Pero la realidad avanza más rápido que los tratados y nos sitúa ante nuevos riesgos que obligan al menos a diseñar soluciones imaginativas antes de que sus efectos sean irreparables. De ahí que las Organizaciones Internacionales avisen

de los daños indiscriminados que pueden provocar las operaciones de desinformación que aún sin uso de la fuerza ya afectan seriamente a procesos democráticos o a bienes tan sensibles para la paz y la estabilidad como la protección del medio ambiente, la seguridad de los ciudadanos o la salud (European Commission, 2019a).

En este sentido, el vicepresidente de la Comisión Europea y alto representante para la política exterior de la Unión, Josep Borrell, ya ha advertido que la desinformación puede matar, en alusión a los mensajes falsos difundidos por internet sobre el Covid-19 y su influencia en el comportamiento de la población frente a los contagios masivos, y en el mismo contexto el Secretario General de la ONU ha alertado sobre el peligro que suponen para la población estas publicaciones fraudulentas y descontroladas. En ambos casos, lo hicieron en las primeras semanas desde la declaración oficial de la pandemia por la Organización Mundial de la Salud (marzo 2020) y en sus respectivas cuentas de *Twitter*.

La OTAN interpreta como ataques las operaciones en el ciberespacio incluyendo la desinformación, un dominio donde ya actúa para defenderse igual que lo hace en tierra, mar y aire. En la Cumbre de Bruselas (NATO, 2018) anunció la creación de equipos especializados en el abordaje de conflictos híbridos para asesorar a estados miembros sobre las repercusiones:

> We announce the establishment of Counter Hybrid Support Teams, which provide tailored, targeted assistance to Allies, upon their request, in preparing for and responding to hybrid activities. We will continue to support our partners as they strengthen their resilience in the face of hybrid challenges. (párr. 21).

Aclarar si la desinformación puede ser un acto de agresión o un ataque no es una cuestión menor, porque de acuerdo con el principio básico de distinción según el artículo 48 del Protocolo 1 (1977) adicional a los Convenios de Ginebra, los ataques sólo deben apuntar a objetivos militares. Sin embargo, la guerra informativa señala principalmente a la población civil, un silogismo cuya conclusión indica que oficialmente la desinformación no debe ser considerada como ataque, si bien sus efectos pueden ser tan graves como si lo fuera. He aquí un problema conceptual que desafía el vigente marco legal internacional y las leyes de la lógica filosófica.

4. LA DESINFORMACIÓN COMO ARMA.

Sería difícil catalogar la desinformación como arma, concepto reservado a la maquinaria militar, quedando así excluida de los usos de la fuerza en el sentido del artículo 2.4 de la Carta de la ONU, ni tampoco como ataque armado según el artículo 51, y de ese modo no procedería invocar el derecho a la legítima defensa al menos en los términos que recoge el capítulo VII. El derecho de los conflictos armados considera armas y en consecuencia objetivo legal de los ataques “aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las

circunstancias del caso una ventaja militar definida", según recoge el artículo 52.2 del Protocolo Adicional 1.

Pero debemos tener en cuenta que es la naturaleza intrínseca de un objeto la que le confiere su condición de arma. Los demás no lo son, pero pueden adquirir esta condición circunstancialmente dependiendo de otros detalles (la ubicación, finalidad o utilización) en un momento preciso (Droege, 2012). Esto nos recuerda que las etiquetas no son definitivas pudiendo pasar de civil a militar y viceversa en cuestión de minutos, y si llegado el caso su neutralización ofrece una ventaja militar definida se convertirán automáticamente en objetivos legítimos.

Aquí está incluida la información (verdadera o falsa) difundida por los medios de comunicación, considerada objeto legal de ataques cuando ayudan al esfuerzo militar o si su destrucción o neutralización suponen una ventaja definida (Schmitt, 2017). Pero este planteamiento no quiere decir que la parte agredida con mensajes falsos no pueda responder adecuadamente para desmontarlos, aunque la magnitud del ataque no alcance un alto nivel de intensidad o su neutralización no llegue a ser una ventaja militar en sentido estricto.

Ocurre casi a diario, y en estos casos la réplica de los estados se articula con acciones hacia dentro y hacia fuera. En el terreno interno, las contramedidas deben estar limitadas por las garantías que ofrecen los derechos humanos para no eliminar los privilegios que disfrutan sus propios ciudadanos como el derecho a la libertad de expresión (salvo en las excepciones contempladas en los tratados para los casos en los que peligre la vida de la nación y cuya existencia haya sido proclamada oficialmente)[3]

Las avalanchas de información maliciosa no pueden considerarse armas en sentido jurídico, pero quedan pocas dudas de que han entrado de lleno en la lista de nuevos métodos de guerra empleados en los conflictos híbridos. El artículo 36 del Protocolo 1 obliga a los Estados a determinar antes de su utilización si una nueva arma, medio o método de guerra estaría autorizado por las normas de conducción de hostilidades, dejando en sus manos la evaluación de su legalidad, pero en el caso que nos ocupa esta duda ya está resuelta desde más de un siglo, desde las primeras codificaciones del derecho de los conflictos armados, porque como dijimos al empezar, la mentira está autorizada como medio legal de guerra.

4.1. Hacia una nueva categoría de conflictos no armados

El Comité Internacional de la Cruz Roja y el Manual de Tallin interpretan que el Derecho Internacional Humanitario es aplicable a las operaciones de desinformación o ciberataques sólo si se producen en el contexto de un conflicto armado, y en ese caso tanto la acción hostil como su respuesta deben respetar

[3]Según lo dispuesto en el artículo 4 del Pacto Internacional de Derechos Civiles y Políticos (1966), o artículo 15 del Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales (1950).

los principios elementales de distinción, precaución, proporcionalidad, necesidad militar y humanidad que limitan la conducción de hostilidades (ICRC, 2019). Sin embargo, hay voces disonantes que proponen nuevas reglas o incluso nuevos tratados para una situación que demanda normas más claras para abordar unos casos que superan el ámbito teórico de los Convenios de Ginebra, porque como se ha apuntado ya, las campañas de desinformación contra un Estado no son operaciones armadas *stricto sensu*.

Estas nuevas modalidades de guerra son en puridad *conflictos no armados* y han venido a inaugurar una categoría no reconocida en el vigente Derecho Internacional Humanitario que hasta ahora exige el uso de la fuerza militar como condición expresa. No existe una definición jurídica sobre la guerra, si bien el Tribunal Penal para la ex Yugoslavia (ICTY, 1995) ofrece una aproximación de gran valor sobre *conflicto armado* como el recurso a la fuerza entre Estados, o la situación que produce violencia armada continuada entre las fuerzas gubernamentales y uno o varios grupos organizados, o entre estos grupos dentro del Estado

Sin cuestionar el peso jurídico de esta aportación, que ha servido de guía para la interpretación de otras situaciones posteriores, no aporta mucho más contenido a la clasificación recogida en los Convenios de Ginebra desde mediados del siglo 20 entre Conflictos Armados Internacionales o No Internacionales, lo que técnicamente impide justificar su existencia si no hay uso de la fuerza. De este modo, la aplicación de las normas de conducción de hostilidades en la ciberguerra o en cualquiera de las operaciones que se desarrollen exclusivamente en internet es incierta cuando no hay violencia armada, a menos que como se ha dicho estén insertas en un conflicto armado convencional o sus consecuencias sean similares.

El derecho todavía permanece en la clasificación entre Conflicto Armado Internacional o no internacional, pero ahora estamos en otra fase evolutiva que parece aconsejar una primera distinción entre conflictos *armados* o *no armados.* Y desde luego los que se apoyan en las campañas de desinformación pertenecen a este último grupo en el que no existe fuerza militar, aunque sí una importante violencia no armada.

> The coronavirus crisis provides insight into challenges that do not typically fall under militarised (use of force) security but could nevertheless destabilise, if not cripple, whole societies. (...) The distinction between peace and war are far less clear now as disinformation and cyberattacks are continuous, rolling campaigns designed to disrupt and destabilize, possibly without end. The grey zone encompasses measures that create destabilisation and conflict below the threshold of overt violence, including disruptive tactics such as disinformation, psychological operations and destabilising legal processes. (Hoogensen, 2020, párr. 5-16).

El mundo gira rápido pero el derecho reacciona lento. Hoy día resulta

complicado incluso distinguir cuándo estamos en guerra porque las diferencias respecto a la paz oficial son más turbias que nunca. Los conflictos no armados, aunque menos visibles, son cada vez más frecuentes y llegan a desarrollarse a mayor escala que los que emplean la fuerza militar. Se camuflan entre los medios de comunicación de masas para fingir la apariencia inofensiva que es la base de su éxito, sobre la base de la confianza del rival (que es la población civil a la que se quiere influir). Es un modo de proceder contrario al de las guerras militares, que se apoyan en el ruido y la opulencia para generar miedo en el enemigo.

Desde luego los *conflictos no armados* tienen un menor efecto destructor que los que utilizan la fuerza, pero probablemente similar potencial desestabilizador. ¿Se puede aplicar la misma norma a dos formas tan distintas de guerra? La Corte Internacional de Justicia (ICJ, 1996), en su Opinión Consultiva sobre la legalidad de la amenaza o el uso de las armas nucleares profetizó la validez de los tratados también para las amenazas que están por llegar y estableció que el derecho de los conflictos armados se debe aplicar: "A todas las formas de guerra y a todos los tipos de armas, tanto las del pasado, las del presente y las del futuro" (párr.86). Y lo hizo quizá arrojando luz sobre la situación actual, inimaginable en la década de los 90.

Actualmente no basta la única referencia a su carácter internacional o local para la clasificación fáctica de los conflictos, sin embargo, el Comité Internacional de la Cruz Roja interpreta la posición de la CIJ como la confirmación de la exclusiva aplicación del derecho humanitario sólo si la ciberguerra o la desinformación, una de las formas de guerra del futuro en la opinión de la Corte, se producen durante un conflicto armado convencional, una de las formas de guerra del pasado.

4.2 La organización de la defensa contra la desinformación. La libertad de expresión como límite

El 69% de los ciudadanos europeos prefiere informarse a través de internet y el 63% se topa con mensajes falsos al menos una vez a la semana (European Commission, 2019b). Muy probablemente le ha ocurrido a usted mismo la última vez que se ha conectado a internet para ver las noticias (quizá hoy, hace sólo unos minutos, cuando un mensaje entrante en su teléfono ha interrumpido la lectura de este texto) y ha tomado por real una información que no lo es, sin darse cuenta. Nuestros hábitos para estar al día sobre asuntos de actualidad han cambiado radicalmente en sólo unos años, dibujando un escenario que la desinformación aprovecha para agrandar su efecto.

La ciberguerra, las guerras híbridas, las operaciones de desinformación plantean dudas sobre su abordaje jurídico a las que instrumentos como la Convención de Budapest (2001) o el ya citado Manual de Tallin (2017) intentan dar respuesta. El primero de ellos marca el inicio de la acción formal contra los delitos en el espacio digital. La llamada Convención de Budapest, o Convenio sobre la ciberdelincuencia elaborado por el Consejo de Europa (2001) es el primer tratado internacional para la lucha contra el crimen en internet, con referencias expresas a la protección de la libertad de expresión ante la debilidad que padece

en la red. Promueve también la defensa en internet de los derechos fundamentales consagrados en el Convenio Europeo de Derechos Humanos (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales para reafirmar "el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras" (Council of Europe, 2001, Preamble).

Por su parte, los Estados han reaccionado con estrategias de defensa para neutralizar campañas contra sus intereses, y en los últimos tres o cuatro años el número de países con regulaciones en este terreno ha aumentado exponencialmente (Bradshaw, Howard & Neudert, 2018) y los sistemas utilizados son diversos, pero básicamente preparan programas e inversiones de seguridad específicos para cortar la influencia de la desinformación en la opinión pública o su interferencia en los resultados electorales. Cada Estado se organiza como puede, individualmente y muchas veces apresuradamente, respondiendo a la urgencia de la amenaza hasta donde alcanza el ejercicio de sus competencias. Pero la desinformación exigirá un abordaje global para neutralizar sus efectos con más garantías, ya que las técnicas en las que se apoya evolucionan con más celeridad que las estrategias o las alianzas entre Estados para la defensa. Hace tiempo que la Asamblea de la ONU trabaja bajo esta premisa, con el convencimiento de que esta lucha no ha hecho más que empezar y la advertencia de que ningún Estado podrá hacer frente en solitario a estas amenazas.

En los últimos años, la Comisión Europea ha respondido a las oleadas de "fake news" con distintos programas que buscan principalmente unidad de acción de los miembros y establecer una pauta común. En este contexto aparecen el Grupo de Alto Nivel sobre fake news y desinformación, el Código de buenas prácticas contra la desinformación (2019) o el Plan de Acción contra la desinformación (2018), basado en cuatro pilares:

> 1. Mejora de la capacidad de las instituciones de la Unión para detectar, analizar y exponer la desinformación. 2. Refuerzo de las respuestas coordinadas y conjuntas a la desinformación. 3. Movilización del sector privado para combatir la desinformación. 4. Aumento de la sensibilización y la capacidad de respuesta de la sociedad. (Comisión Europea, 2018, párr. 3).

4.3 La defensa contra la desinformación. Empoderando a los ciudadanos

Si el objetivo final es evitar el efecto de los mensajes falsos sobre la opinión pública, parece obvio que también hay que actuar sobre los consumidores de información para prevenirles. Y aquí encontramos la paradoja de la desinformación. Por un lado las organizaciones internacionales y los gobiernos señalan la baja calidad del periodismo y la poca conciencia crítica de los ciudadanos, como parte del problema:

> La crisis financiera y el avance de nuevas formas de medios de comunicación digital han

> planteado importantes desafíos para el periodismo de calidad, que han conllevado una disminución del pensamiento crítico entre el público, haciéndole más susceptible a la desinformación y a la manipulación. (Parlamento Europeo, 2016, párr. 2).

Pero por otro, en demasiadas ocasiones son los poderes públicos los responsables en la idiotización de los ciudadanos, a quienes vigilan más que protegen para controlar su actividad. Frecuentemente, sus programas para repeler los mensajes contrarios a sus intereses erosionan la libertad de expresión de los ciudadanos. La Asamblea General de la ONU insiste en que las medidas de protección contra la desinformación no deben colisionar con la obligada protección de los derechos humanos porque no son objetivos contrapuestos, sino que se complementan y se refuerzan mutuamente:

> [La Asamblea General] condena inequívocamente las medidas adoptadas por los Estados, vulnerando el derecho internacional de los derechos humanos, con miras a impedir u obstaculizar deliberadamente, como de hecho ocurre, el acceso a información en línea o en otros medios o su divulgación, y que tienen el objetivo de menoscabar la labor que realizan los periodistas de informar al público, incluidas las medidas cuyo fin es restringir, bloquear o desactivar indebidamente sitios web de medios de comunicación… (Asamblea General de la ONU, 2020b, pár. 12).

Las Organizaciones Internacionales en general advierten sobre la censurable acción de los gobiernos que combaten la desinformación con acciones desmesuradas más orientadas a la interrupción de los derechos fundamentales que a su protección, y recuerda los límites que deben observar. Cuando se olvida la protección de las garantías jurídicas los civiles nos convertimos doblemente en víctimas, primero por la manipulación informativa en sí, con mensajes que llegan desde fuera y segundo por los recortes de derechos de los propios poderes públicos, que son los encargados de protegerlos.

La vigilancia o limitación del uso de internet, las medidas de control sobre las publicaciones de los particulares y otras muchas empoderan de manera fraudulenta a los gobiernos, amparados en la necesidad de sostener el ataque. Deben combatir las campañas de desinformación sin lesionar la libertad de expresión, porque sería tanto como colaborar con sus pretensiones para debilitar las instituciones públicas o interferir en los resultados electorales (European Parliament, 2019).

Entre las alertas que continuamente lanzan las Organizaciones Internacionales debemos incluir la defensa de la privacidad, condición fundamental para el disfrute y ejercicio de la mayoría de los derechos y libertades recogidas en el Convenio Europeo de Derechos Humanos. Así se posiciona el Comité de ministros del Consejo de Europa (Council of Europe, 2018):

> The rule of law is a prerequisite for the protection and promotion of the exercise of human rights and for pluralistic and participatory democracy. Member States have the obligation to refrain from violating the right to freedom of expression and other human rights in the digital environment. (párr. 6).

En general, llamadas de este tipo son habituales en la misma medida en que también lo son las cortapisas al derecho de los ciudadanos a la libertad de expresión. Se trata de una acción contradictoria en sí misma, que por un lado dificulta el ejercicio de los derechos fundamentales a la vez que promueve su defensa. La prioridad radica en la regulación de los contenidos que circulan por internet, sin entrar en otras limitaciones que puedan limitar derechos de los ciudadanos. Tras la declaración de la pandemia por el COVID 19 (marzo 2020) alrededor de un centenar de gobiernos de todo el mundo declararon situaciones jurídicas excepcionales, que limitaban los derechos fundamentales de las personas. Sin embargo, en la mayoría de los casos no han notificado a las Naciones Unidas la adopción de estas medidas, como lo exige el Pacto Internacional de Derechos Civiles y Políticos, y muchas de ellas carecen de cláusulas de extinción (UNESCO, 2020, p.11).

Si bien las limitaciones temporales al ejercicio de los derechos humanos por motivos de salud pública pueden ser legítimas en virtud del derecho internacional, en muchos casos estas medidas han tenido repercusiones desproporcionadas, y no cumplen los requisitos establecidos para la restricción de estos derechos. La queja recuerda que para que la limitación de un derecho humano sea legítima, el derecho internacional requiere que 1) se encuentre en la ley; 2) sea necesaria para alcanzar el objetivo propuesto, y 3) cumpla un propósito legítimo, de acuerdo con el Pacto Internacional de Derechos Civiles y Políticos.

Paralelamente al aumento de la desinformación y a las estrategias oficiales para evitarla, la sociedad civil se ha organizado utilizando precisamente la facilidad que ofrece internet. Y lo hace básicamente para denunciar el aumento de cortes en la red que menoscaban la libre circulación de ideas

> "An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information" (Accesnow.org, 2021, par 7).

Sin olvidarnos de las iniciativas ciudadanas para deshacer bulos o eliminar prejuicios infundados, que serán objeto de otro estudio. Sólo nombraremos ahora la Red Internacional de Verificación, una asociación sin ánimo de lucro integrada principalmente por periodistas para verificar noticias y eliminar bulos, La International Fact-Checking Network (*IFCN*, por sus siglas en inglés) es una unidad del *Instituto Poynter* que reúne a más de 50 miembros en todo el mundo y trabaja desde 2015. Y como ella, cientos de organizaciones

similares rastrean cada minuto el espacio virtual a la caza de mensajes maliciosos para devolver la verdad al lugar que nunca debió perder, o, mejor dicho, al que nunca ocupó ni en la guerra ni en la paz.

CONCLUSIONES

¿Estamos en guerra o en tiempo de paz? Terminamos este estudio sin una respuesta para esta cuestión elemental. A usted, ¿qué le parece? Al menos, resulta claro que estamos sumidos en una suerte de división en bloques similar al que hubo durante la llamada Guerra Fría llamado ahora *ciberguerra fría* por los estrategas y empresas especializadas en seguridad digital que prevén un aumento inmediato de las campañas de propagación de desinformación entre los espacios que representan Rusia, China, Estados Unidos y la Unión Europea. Rusia opta por mensajes para debilitar al rival, mientras que China prefiere el fortalecimiento propio, con proclamas que agrandan sus éxitos (Mateos, 2020).

Se habla también de guerra informativa, de guerra sin reglas por ser enfrentamientos sin normas específicas para su abordaje, y hasta de guerra en la sombra (Sciutto, 2019). Más allá de la etiqueta, que como dijimos al principio no es lo que nos ocupa, significa que se está desarrollando ahora mismo, mientras usted lee inconsciente de que ocurre porque no hay declaración formal ni escenarios cruentos, lo que la ha convertido en la modalidad más atractiva de guerra (ICRC, 2019, p.3) preferible frente a los enfrentamientos armados convencionales.

Pongamos un ejemplo: Como consecuencia de la pandemia de la l COVID 19, la Organización Mundial de la Salud ha tenido que poner en marcha un plan específico contra la desinformación para desmontar los mensajes propagados a gran escala que causan alarma en la población o ponen en riesgo su salud y ha mostrado su preocupación por una nueva pandemia: *la infodemia* (World Health Organization, 2020, p.2) La exagerada difusión de informaciones falseadas o sin fundamento sobre esta crisis sanitaria, como en tantas otras ocasiones, tiene un efecto demoledor en la confianza que los ciudadanos depositamos sobre las instituciones que deben proponer soluciones.

Este es el objetivo de la desinformación, dañar la confianza en las instituciones del oponente a través de la configuración de la opinión pública sirviéndose de mensajes maliciosos. Una vez inoculado, el mensaje representa un caballo de Troya en las tripas del sistema propio, una enfermedad autoinmune de desestabilización sin utilizar los métodos habituales de guerra. Cuando no se puede alterar la voluntad de los dirigentes del Estado, se ataca la de los ciudadanos.

La desinformación prolifera en un entorno de manipulación formal de los mensajes y de baja calidad periodística, ayudada por la escasa capacidad ciudadana para bloquearlos mediante el ejercicio del pensamiento crítico. Por eso hoy es tan necesario como siempre sostener el periodismo de calidad basado en la buena fe y en la pluralidad de fuentes porque representa una práctica comprometida con los derechos de los ciudadanos. Necesitamos medios de comunicación independientes con el apoyo firme y desinteresado de los gobiernos (Council of Europe, 2019, párr. 12) para garantizar el acceso de los ciudadanos a una información de calidad junto con la necesaria abstención de

utilizarlos para fines particulares, como parte de las obligaciones positivas que imponen los tratados. Los instrumentos que afrontan este problema, algunos de los cuales hemos repasado, apenas pasan de ser declaraciones de intenciones, actos sin fuerza normativa o de *soft law*

La desinformación se propaga sin demasiadas herramientas en su contra, utilizando de manera espuria los cauces de la libertad de expresión. En efecto, si repasamos los tratados internacionales que sí tienen capacidad jurídica vinculante comprobaremos que protegen la difusión de información en sentido amplio, dentro de la defensa del derecho a la libertad de expresión, aunque sin exigir que sea información veraz y verificable. El artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (1966) protege la libertad de buscar, recibir y difundir informaciones e ideas de toda índole sin la censura de los poderes públicos y sin entrar en más consideraciones sobre la veracidad de los mensajes.

En similares términos se expresa el artículo 13 de la Convención Americana de Derechos Humanos (1969) que no exige que sean mensajes reales o al menos no maliciosos para protegerlos bajo el paraguas del derecho. Una lectura interesada de estas provisiones podría concluir que defienden la difusión de mensajes sin más filtros, sean verdaderos o falsos, y sin que los poderes públicos puedan inmiscuirse salvo que peligre la vida de la nación, en cuyo caso podrían suspender esas garantías para todos los mensajes, tanto veraces como falsos. Probablemente la lucha contra la desinformación tendría otras herramientas si estos instrumentos blindaran sólo la información veraz. Entre las pocas excepciones a esta pauta general se encuentra la Constitución Política de Colombia (1991) que cita así: "Garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial" (art. 20).

En similares términos se expresa el artículo 24 de la Constitución Española (1978) que reconoce el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión. La verdad tiene pocos defensores tanto en la paz como en la guerra. El derecho de los conflictos armados protege la mentira como herramienta legal para la guerra, pero no la de la verdad. Contempla el uso válido del engaño, pero aún ignora el valor de la libertad de expresión.

REFERENCIAS BIBLIOGRÁFICAS

I. Althius, J., & Strand, S. (2018). Fake News, a roadmap. NATO Strategic Communications Centre of Excellence, Riga. Tomado de https://www.stratcomcoe.org/fake-news-roadmap Revisado 30 Junio 2021.

II. Barrancos, D. (2019). Las elecciones más hackeables de Europa. En *Thiber Digest.* Informe mensual de ciberseguridad, (11). Tomado de https://thiber.org/wp-content/uploads/2019/07/Numer

o_11_Julio_optimizado.pdf, Revisado 30 junio 2021.

III. Bothe, M. (1982). N*ew Rules for Victims of Armed Conflicts. Commentary on the Two 1977 Protocols. Additional to the Geneva Conventions of 1949*. Martinus Nijhoff Publishers, Dordrecht.

IV. Bradshaw, S., Howard, P. N. & Neudert, L. M (2018). Government Responses to Malicious Use of Social Media. NATO Strategic Communications Centre of Excellence, Riga. Tomado de https://www.stratcomcoe.org/government-responses-malicious-use-social-media Revisado 30 Junio 2021.

V. Cleary, T. (2008). *El Arte de la Guerra, Sun Tzu*. Versión con comentarios de Thomas Cleary. Madrid, ed. EDAF. Original publicado en el siglo V a.c.

VI. Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross, 94*(886). Tomado de https://international-review.icrc.org/articles/get-my-cloud-cyber-warfare-international-humanitarian-law-and-protection-civilians Revisado 30 Junio 2021

VII. Fundéu RAE. (28 de septiembre de 2017). *Noticias falsas o falseadas, mejor que fake news*. Fundéu RAE, buscador urgente de dudas. Tomado de https://www.fundeu.es/recomendacion/noticia-falsa-falseada-fake-news/ Revisado 30 junio 2021.

VIII. Gutiérrez, C. y Cervell M. J. (2012). *El Derecho Internacional en la Encrucijad*a. Madrid, ed. Trotta.

IX. Haiden, L. (2018) Tell me lies, tell me sweet lies. *Fake News, a roadmap.* NATO Strategic Communications Centre of Excellence Riga, 7-14. Tomado de https://stratcomcoe.org/cuploads/pfiles/fake_news_book_final_full_version.pdf Revisado 30 junio 2021

X. Hoogensen, G. (2020, 20 May). *Coronavirus, invisible threats and preparing for resilience. NATO Review.* Tomado de

https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html

XI. Levin, D. H. (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral. *International Studies Quarterly*, *60*, (60). Issue 2, June 2016, pp. 189–202. Tomado de https://igcc.ucsd.edu/_files/great-powers/gp_reading_levin.pdf.

XII. Lieber, F. (1863). *Instructions for the Government of Armies of the United States in the Field. International Committee of the Red Cross*. Tomado de https://ihl-databases.icrc.org/ihl/INTRO/110 Revisado 30 Junio 2021

XIII. Mateos, I. (15 de enero de 2020). EE.UU y Rusia miden sus fuerzas en una guerra fría cibernética Observatorio de Inteligencia, Seguridad y Defensa. *Revista digital*. Tomado de https://observatorio.cisde.es/actualidad/ee-uu-y-rusia-miden-sus-fuerzas-en-una-guerra-fria-cibernetica/ Revisado 30 junio 2021

XIV. Panetta, K. (Octubre 03 de 2017). *Smarter with Gartner*. Gartner Top Strategic Predictions for 2018 and beyond. Tomado de https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/

XV. Payne, K. (2005). The media as an instrument of war. *Parameters, 35(1).* United States Army War College. Spring 2005. Tomado de https://press.armywarcollege.edu/parameters/vol35/iss1/10 Revisado 30 junio 2021.

XVI. Pizarroso, A. (2007). *Periodismo de guerra*, Madrid, Ed. Síntesis.

XVII. Schmitt, M. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross, 84*(846), 377-378.

XVIII. Schmitt, M. (2017). *Tallinn manual 2.0 on the international law applicable to cyber warfare.* Cambridge University Press.

XIX. Sciutto, J. (2019). *The Shadow War: Inside the Modern-Day Undeclared Battles Waged*

Against America. Harper Collins Publisher.

XX. Soroush, V., Deb, R. & Sinan, A. (2018). The spread of true and false news online. *Science 09*(359), pp. 1146-1151. Tomado de https://science.sciencemag.org/content/359/6380/1146 Revisado 30 Junio 2021.

XXI. Symantec. (2019). Internet Security Threat Report Volume 24. Tomado de https://docs.broadcom.com/doc/istr-24-2019-en Revisado 30 Junio 2021.

XXII. https://www.accessnow.org. (2021) Revisado el 30 Junio 2021.

REFERENCIAS JURISPRUDENCIALES

Documentos de las Naciones Unidas Asamblea General

XXIII. ONU (1945a) Carta de San Francisco. Tomado de https://www.un.org/es/about-us/un-charter Revisado el 30 Junio 2021.

XXIV. ONU (1945b) Estatuto de la Corte Internacional de Justicia. Tomado de https://www.un.org/es/about-us/un-charter/statute-of-the-international-court-of-justice Revisado el 30 Junio 2021.

XXV. ONU (1970) Asamblea General de la Organización de Naciones Unidas. Tomado de A/RES/2625(XXV) Revisado el 30 Junio 2021

XXVI. ONU (1974) Asamblea General de la Organización de Naciones Unidas. Tomado de A/RES 3314 (XXIX). Revisado el 30 Junio 2021

XXVII. ONU (2021) Asamblea General de la Organización de Naciones Unidas. Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. tomado de A/65/201. Revisado el 30 Junio 2021.

XXVIII. ONU (2010) Asamblea General de la Organización de Naciones Unidas. Tomado de A/65/201. Revisado el 30 Junio 2021.

XXIX. ONU (2018) Asamblea General de la Organización de Naciones Unidas. Tomado de

A/RES/73/27 Revisado el 30 Junio 2021

XXX. ONU (2020a) Asamblea General de la Organización de Naciones Unidas. Tomado de A/RES/74/147. Revisado el 30 Junio 2021.

XXXI. ONU (2020b) Asamblea General de la Organización de Naciones Unidas. Tomado de A/RES/74/157. Revisado el 30 Junio 2021.

XXXII. ONU (1991) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/688(1991) Revisado el 30 Junio 2021.

XXXIII. ONU (1991) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/713(1991) Revisado el 30 Junio 2021

XXXIV. ONU (1992) Consejo de Seguridad de la Organización de Naciones Unidas. tomado de S/RES/731(1992). Revisado el 30 Junio 2021.

XXXV. ONU (1992) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/748(1992). Revisado el 30 Junio 2021

XXXVI. ONU (1993) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/808(1993). Revisado el 30 Junio 2021

XXXVII. ONU (1994) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/940(1994). Revisado el 30 Junio 2021.

XXXVIII. ONU (1994) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/949(1994). Revisado el 30 Junio 2021

XXXIX. ONU (2011) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/1973(2011). Revisado el 30 Junio 2021.

XL. ONU (2015) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/2220 (2015). Revisado el 30 Junio 2021.

XLI. ONU (2019) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/2482(2019). Revisado el 30 Junio 2021.

XLII. ONU (2019) Consejo de Seguridad de la Organización de Naciones Unidas. Tomado de S/RES/2490(2019). Revisado el 30 Junio 2021

OTROS DOCUMENTOS DE FUENTES OFICIALES Y ORGANIZACIONES INTERNACIONALES

XLIII. Council of Europe (2001) Convention on Cybercrime. Tomado de Council of Europe - Convention on Cybercrime (ETS No. 185) Revisado el 30 Junio 2021.

XLIV. Comisión Europea. (2018). Plan de Acción contra la Desinformación. Tomado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018JC0036&from=en Revisado 30 Junio 2021.

XLV. Parlamento Europeo. (2016). Resolución sobre la comunicación estratégica de la Unión para contrarrestar la propaganda de terceros en su contra. Tomado de https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_ES.pdf?redirect Revisado 30 Junio 2021.

XLVI. Council Of Europe. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Tomado de https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c Revisado 30 Junio 2021.

XLVII. Council of Europe. (2019). Declaration by the Committee of Ministers on the financial sustainability of quality journalism in the digital age. Tomado de https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4d Revisado 30 Junio 2021.

XLVIII. Council of Europe. (2018). Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. Tomado de https://rm.coe.int/1680790e14 Revisado 30 Junio 2021.

XLIX. International Committee of the Red Cross -ICRC-. (1874).

Project of an International Declaration concerning the Laws and Customs of War. Tomado de https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=11CC9AB4930720C4C12563CD0051555C Revisado 30 Junio 2021.

L. International Committee of the Red Cross -ICRC-. (2005). Customary IHL, art. 57. Ruses of war. Tomado de https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule57#Fn_5496F01B_00001. Revisado 30 Junio 2021.

LI. International Committee of the Red Cross -ICRC-. (2015). International humanitarian law and the challenges of contemporary armed conflicts. tomado de https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts Revisado 30 Junio 2021.

LII. International Committee of the Red Cross -ICRC-. (2019). International Humanitarian Law and Cyber Operations during Armed Conflicts Position paper. Tomado de https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts#gs.ke2c5o Revisado 30 Junio 2021.

LIII. European Commission. (2018b). Fake News and Disinformation Online. Tomado de https://data.europa.eu/data/datasets/s2183_464_eng?locale=en Revisado 30 Junio 2021.

LIV. European Commission. (2019a). Código de buenas prácticas de la Unión en materia de desinformación. (versión en español). Tomado de https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation Revisado 30 Junio 2021.

LV. European Commission. (2019b). Code of Practice on Disinformation. Tackling online disinformation. Tomado de Disinformation: A threat to democracy - Brochure | Shaping Europe's digital future. Revisado 30 Junio 2021.

LVI. European Parliament. (2019). Resolution on foreign electoral interference and disinformation in national and European democratic processes. (2019/2810(RSP)). Tomado de https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.html Revisado 30 Junio 2021

REFERENCIAS NORMATIVAS

LVII. España. D. 14/2019. Por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Tomado de Documento BOE-A-2019-15790 Revisado 30 Junio 2021.

LVIII. North Atlantic Treaty Organization -NATO-. (2018). Brussels Summit Declaration. Tomado de https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21 Revisado 30 Junio 2021.

LIX. North Atlantic Treaty Organization -NATO-. (2020). Coronavirus, invisible threats and preparing for resilience. *NATO Review*. Tomado de Coronavirus, invisible threats and preparing for resilience Revisado 30 Junio 2021.

LX. UNESCO. (2020). Periodismo, libertad de prensa y COVID-19. *Tendencias mundiales en libertad de expresión y desarrollo de los medios de comunicación.* Tomado de https://en.unesco.org/sites/default/files/unesco_covid_brief_es.pdf Revisado 30 Junio 2021.

LXI. World Forum For Democracy (2019) Is democracy in danger in the information age? Tomado de World Forum for Democracy 2019 Revisado 30 Junio 2021.

LXII. World Health Organization. (2 de febrero de 2020). Novel Coronavirus (2019-nCoV). Situation Report. Tomado de https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf Revisado 30 Junio 2021.

Documentos Tribunales Internacionales

LXIII. International Criminal Tribunal for the former Yugoslavia - ICTY-. (1995). Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction. The Prosecutor v. Dusko Tadic, IT-94-1-A. Tomado de Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction Revisado 30 Junio 2021.

LXIV. International Court of Justice - ICJ-. (1996). Legality of the threat or the use of nuclear weapons. Advisory Opinion. Tomado de https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf Revisado 30 Junio 2021.

Referencias Complementarias.

LXV. Corte Suprema de Justicia. (2014, 20 de agosto). Sentencia C-593/14 (Jorge Ignacio Pretelt Chaljub, M. P.). Tomado de https://bit.ly/36v1n1l. Revisado el 30 Junio 2021.

LXVI. Corte Interamericana Derechos Humanos (2013, 22 agosto) Sentencia Caso Mémoli v. Argentina. Tomado de http://www.corteidh.or.cr/docs/casos/articulos/seriec_265_esp.pdf Revisado el 30 Junio 2021.

LXVII. Corte Interamericana Derechos Humanos (2013, 3 septiembre) Sentencia Caso Vélez Restrepo y familiares v. Colombia, Tomado de https://corteidh.or.cr/docs/casos/articulos/seriec_248_esp.pdf Revisado el 30 Junio 2021.

LXVIII. Ingatidou S. (2019) EU–US Cooperation on Tackling Disinformation,*Catham House.* The Royal Institute of International Affairs. Tomado de https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf Revisado 30 Junio 2021.

LXIX. The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland (2015) Press Release, *The Military Doctrine of the Russian Federation*. Tomado de THE MILITARY DOCTRINE OF THE RUSSIAN FEDERATION Revisado 30 Junio 2021.

LXX. North Atlantic Treaty Organization -NATO-. (2016). Warsaw Summit Communiqué. Tomado de https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Revisado 30 junio 2021.

LXXI. International Committee of the Red Cross -ICRC-. (2017). Tomado de The Potential Human Cost of Cyber Operations. Revisado 30 junio 2021.

LXXII. International Committee of the Red Cross -ICRC-. (1987). Tomado de Commentaries to Additional Protocol 1. Revisado 30 Junio 2021.

LXXIII. Suárez Serrano Ch. (2017) *Periodismo y Derecho Internacional Humanitario, un análisis para el siglo 21*. Madrid, Dykinson.

LXXIV. European Commission. (2018a). Experts appointed to the High-Level Group on Fake News and online disinformation | Shaping Europe's digital future. Tomado de https://digital-strategy.ec.europa.eu/en/news/experts-appointed-high-level-group-fake-news-and-online-disinformation Revisado 30 Junio 2021.

LXXV. European Commission. (2018c) Democracy and Elections. Special Eurobarometer 477. Taomado de https://coinform.eu/wp-content/uploads/2019/02/Euro-Barometer.pdf Revisado 30 junio 2021.